

OCT 04 2005

PAGE 1/16 \* RCVD AT 10/4/2005 4:10:42 PM [Eastern Daylight Time] \* SVR:USPTO-EFXRF-6/27 \* DNIS:2738300 \* CSID:512 703 1250 \* DURATION (mm:ss):09:28

## **II. RELATED APPEALS AND INTERFERENCES**

A Notice of Appeal has been filed for the following application, which shares a common specification with the application currently on appeal: 09/752,072 Notice of Appeal filed 2/10/05. However, because dissimilar art is cited in the present application and the above-mentioned related application, Appellants do not believe that the outcome of this appeal will have any bearing on the Board's decision on the related appeals. No other appeals or interferences are known which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

## **III. STATUS OF CLAIMS**

Claims 1-3 and 5-26 stand finally rejected. No claims have been allowed, withdrawn, or objected to. Claim 4 has been canceled. Claims 1-3 and 5-26 are being appealed.

## **IV. STATUS OF AMENDMENTS**

No amendments to the claims have been filed subsequent to their final rejection. The Claims Appendix attached hereto reflects the current state of the claims.

## **V. SUMMARY OF CLAIMED SUBJECT MATTER**

Appellant's claimed subject matter includes a system and method for identifying and binding a process over a heterogeneous network comprising a network server, a network client and a network host. (Specification – page 8, lines 3-25 and Fig. 1). In addition, the Appellant's claimed subject matter includes a computer-usable carrier medium having program instructions which are executable on a computational device for performing such a method. (Specification – page 34, lines 22-29). The claimed system, method and carrier medium may include a network server, which is adapted to receive a payload from a network client, where the payload comprises a request for process execution associated with a task. (Specification – page 14, line 23 to page 15, line 3; page 16, line 22 to page 17, line 5; and page 22, lines 12-29). In addition, the network server is adapted to evaluate the payload, create an agent from the payload, and forward the agent to a network host for process execution associated with the agent. (Specification – page 23, lines 1-18; page 30, line 28 to page 31, line 27). In a particular embodiment of the invention, the network host is unknown to and dissimilar from the network client. In other words, the

network host and network client remain anonymous to each other throughout the identifying and binding process. (Specification – page 17, lines 10-14; page 19, lines 15-24).

#### **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

1. Claims 1-3, 5-12, 17, 25 and 26 are rejected under 35 U.S.C § 103(a) as being unpatentable over U.S. Patent No. 6,112,225 to Kraft et al. (hereinafter referred to as “Kraft”) in view of U.S. Patent No. 6,421,653 to May (hereinafter referred to as “May”).
2. Claims 13-16 and 18-24 are rejected under 35 U.S.C § 103(a) as being unpatentable over Kraft and May, as applied to claims 1, 12 and 17, and further in view of U.S. Patent No. 6,732,141 to Ellis (hereinafter referred to as “Ellis”).

#### **VII. ARGUMENT**

The contentions of the Appellant with respect to the ground of rejection presented for review, and the basis thereof, with citations of the statutes, regulations, authorities, and parts of the record relied on are presented herein for consideration by the Board.

##### **A. Patentability of Claims 1-3, 5-12, 17, 25 and 26:**

1. Kraft and May each fail to teach or suggest a system (claim 1), computer usable carrier medium (claims 25-26) or method (claims 12 and 17) in which a network server is adapted to: (i) create an agent from a payload, which is received from a network client and includes a request for process execution associated with a task, and (ii) forward the agent to a network host for process execution, where the network host is unknown to and dissimilar from the network client.

Independent claim 1 recites:

A system for identifying and binding a process, said system comprising a network server adapted to receive a payload from a network client over a network, wherein the payload comprises a request for process execution associated with a task, and wherein the server is further adapted to evaluate the payload, create an agent from the payload, and forward the agent to a network host, unknown to and dissimilar from the network client, for process execution associated with the agent.

The presently claimed case provides a system and method in which computing resources can be used efficiently within network-connected devices. For instance, in a network of servers, clients and hosts, one or more "client" computers may require processing of a task, whereas one or more "host" computers may wish to devote unused computing resources to the execution of a task. The network server functions as an intermediary between the network clients and the network hosts. For example, a network server may receive a payload from a network client. In some cases, the payload may simply be a request to execute a task. In other cases, the payload may include a set of programming instructions (302, Fig. 3) used to process data, a data set (304), a task ID (305), containing security permissions (306), and a financial data set (308). Once the payload is received, the network server may evaluate the payload (e.g., by authenticating the payload, inspecting the payload for conformance to network protocols, etc.) and create an agent from the payload. The agent is a software process configured to perform the task. The network server may forward the agent to a network host for process execution of the task. However, in order to provide secure and anonymous processing, the network server does not disclose the identity of the computer (i.e., network client) requesting process execution or the computer (i.e., network host) performing the process execution. In this manner, the network client and network host remain unknown to and dissimilar from each other. In other words, the network client and network host are different entities, whose identities are maintained anonymous. (See, relevant portions of the Specification, including those set forth in the Summary Section of this Appeal).

Unlike the presently claimed case, Kraft and May each fail to disclose a system, computer-usable carrier medium or method in which anonymity is maintained between a first computer (e.g., a network client) requesting process execution of a task and a second computer (e.g., a network host) performing the process execution.

Statements in the Final Office Action admit that Kraft "does not expressly disclose that the network client and the network host are anonymous from each other." (Final Office Action, page 5). However, further statements suggest that such anonymity may be found within May, and that it would be obvious to combine May's anonymous automated auction method with Kraft's automated auction in order to better ensure fairness. (See, Final Office Action, page 5). As described in more detail below, Kraft and May each fail to disclose the anonymous process set forth in the presently claimed case, and more specifically, cannot be combined or modified to do so.

May discloses "systems, methods, and computer program products that provide for electronic trading based on the client/server model, including a central processing center (i.e., server) having multiple server modules and a plurality of individual trader workstations (i.e., clients), all of which are operationally interconnected, preferably via an Internet-protocol network." (May, column 5, lines 48-55). In Fig. 1, for example, May discloses "a trading system 10... [including] a central processing center 12 which is in communication with the client sites 14 via one or more of a variety of Internet protocol based networks 16." (May, column 11, line 65 to column 12, line 2). Within trading system 10, "a user's own desktop computer which is connected to the client's internal data network may function as a trader workstation 20 and run the Java-based software of the present invention to enable interaction with other trader workstations 20 via the central processing center 12." (May, column 12, lines 21-26). Beginning in column 16, May describes how a user at trader workstation 20 may connect to the central processing center 12 to access features of the system 10, which enable the user to monitor and control their trading within system 10. (See, e.g., May, column 16, line 28 to column 17, line 53).

For example, when a user wishes to place an order (i.e., initiate a trade), the user selects an order from the market details interface (302, Fig. 15) displayed on the user's trader workstation. The market details interface enables a trader/user to view essentially all the orders in the market for a particular instrument, including bids and offers from other traders/counterparties. Once selected, the user's order is entered into the system 10 and placed in a queue based on price and time received. (See, e.g., May, column 36, line 45 to column 38, line 37, column 6, lines 16-62 and column 12, lines 27-46). Once the order is placed in the system, an "execution notification message 340, as illustrated in Fig. 18, is sent to both counterparties, describing the transaction and the names of the counterparties... system 10 ensures that both users receive the message before the trade is finally completed." (May, column 38, lines 36-43).

Statements in the Final Office Action suggest that May discloses a system in which anonymity between buyers and sellers is maintained (Final Office Action, page 5). As noted above, however, May specifically teaches that the identities of the buyers and sellers (i.e., the counterparties) are disclosed to one another before a trade is finally completed. Therefore, if one were to assume that a "buyer" requesting a trade is somehow equivalent to a "network client" requesting process execution of a task, and a "seller" providing the trade is somehow equivalent to a "network host" performing the process execution, then May absolutely fails to teach anonymity between a network client and a network host.

2. There is no motivation to combine or modify the teachings of the cited art to provide a network server adapted to: (i) create an agent from a payload, which is received from a network client and includes a request for process execution associated with a task, and (ii) forward the agent to a network host for process execution, where the network host is unknown to and dissimilar from the network client.

To establish a case of *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (C.C.P.A. 1974); MPEP 2143.03. Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed.Cir. 1988); *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992); MPEP 2143.01. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination [or modification]. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990); MPEP 2143.01.

Kraft and May each fail to suggest a desirability for the presently claimed anonymity between a network client and a network host, and therefore, cannot be combined or modified to do so.

For instance, statements in the Final Office Action suggest that Kraft provides teaching for "security considerations (col. 10, lines 5-35), but does not expressly disclose that the network client and network host are anonymous from each other." (Final Office Action, page 5). As such, the Examiner appears to suggest that the "security considerations" disclosed by Kraft may imply or provide motivation for a system and method, which maintains anonymity between network clients and network hosts. This is simply not the case. In fact, upon reviewing the suggested "security considerations" provided by Kraft, a skilled artisan would come to the conclusion that such anonymity is not only undesirable, but counterproductive to the security considerations proposed by Kraft. For example, Kraft suggests that one "option is to require digital signatures for imported tasks... [so that] the peripheral computers can verify that received programs and subtasks originate from a trusted source." (Kraft, column 10, lines 22-25). As another security measure, Kraft suggests "requiring authentication for communication between peripheral and coordinating computers." (Kraft, column 10, lines 25-27). Clearly, Kraft does not wish to maintain anonymity between the peripheral and coordinating computers, and therefore, provides no motivation to do so.

Like Kraft, May also fails to suggest a desirability for the presently claimed anonymity between a network client requesting process execution of a task and a network host performing the process execution. Statements in the Final Office Action suggest that May teaches that "anonymity between buyers and sellers is maintained." (Final Office Action, page 5). However, as explained above in Argument 1, anonymity between buyers and sellers is not maintained, since May specifically states that the names of the buyers and sellers (i.e., the counterparties) are disclosed to one another before the trade is finally completed (See, May, column 38, lines 36-42). May stresses that the system "ensures that both users receive the [execution notification] message before the trade is finally completed." (May, column 38, lines 42-43, emphasis added). The only anonymity taught by May is "for an automated system for distributing anonymous price and position information" (May, column 5, lines 20-25). However, distributing anonymous price and position information is by no means equivalent to maintaining anonymous identities, nor does it suggest a desirability for doing so.

Since Kraft and May each fail to teach, suggest or even provide desirability for the presently claimed anonymity between a network client and a network host, the teachings of Kraft and May cannot be combined or modified to do so.

**3. The Examiner has failed to adequately support and/or establish a *prima facie* ground of obviousness.**

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all claim limitations. MPEP § 2143. None of these three criteria have been met by the Examiner in the present case. First of all, no suggestion or motivation to modify the cited references can be found within the cited references to teach or suggest the aforementioned limitations of present claims 1, 12, 17, 25 and 26, as explained above in Argument 2. The criterion of a reasonable expectation of success cannot be met if no teaching, suggestion or motivation exists, because there is then nothing at which to be successful. Finally, none of the cited art, either alone or in combination, teaches all of the limitations of claims 1, 12, 17, 25 and 26, as explained above in Arguments 1 and 2. The third criterion recited above has therefore also not been met, and a *prima facie* case of obviousness has not been established.

### Conclusion

As explained in Arguments 1-3 above, at least some limitations of claims 1, 12, 17, 25 and 26 are not taught or suggested by the cited art. Furthermore, there is no teaching, suggestion or motivation to modify the cited art to teach the limitations of these claims. For at least the reasons set forth above, claims 1, 12, 17, 25, 26, and all claims dependent thereon, are patentably distinct over the cited art. As such, the rejection of claims 1-3, 5-12, 17, 25 and 26 under 35 U.S.C. § 103(a) is asserted to be erroneous.

#### **B. Patentability of Claims 13-16 and 18-24:**

Because claims 13-16 and 18-24 include limitations similar to those included within Independent claims 12 and 17, the arguments presented above for patentability of claims 12 and 17 apply equally to claims 13-16 and 18-24, and are herein incorporated by reference. In addition to the arguments presented above with respect to 13-16 and 18-24, arguments are provided below to further establish the patentability of the current claims under 35 U.S.C. §103(a).

- 1. The cited art fails to teach or suggest a method for identifying and binding a process, where the method includes evaluating a payload by authenticating the payload and checking the payload for conformance to a set of protocols.**

Dependent claims 13 and 18 recite “[t]he method as recited in claim 12, wherein evaluating a payload comprises authenticating the payload and checking the payload for conformance to a set of protocols.” Statements in the Final Office Action admit “Kraft and May do not expressly disclose evaluating a payload comprises authenticating the payload and checking the payload for conformance to a set of protocols.” (Final Office Action, page 6). However, further statements in the Final Office Action suggest that “Ellis teaches this limitation (col. 11, line 53 – col. 12, line 20). The Appellant respectfully disagrees, for at least the reasons set forth in more detail below.

The Examiner suggests that teaching for the abovementioned limitation may be found in columns 11 to 12 of Ellis. The cited passage describes a signaling device, which provides a signal “to indicate the user PC’s availability 14 for network use” and “its specific... configuration” (Ellis, column 11, line 53 to column 12, line 20). However, a “signal” indicating a PC’s configuration and availability for network use is not equivalent to the presently claimed “payload” (which includes a request for process execution



of a task) or the presently claimed method for evaluating a payload. Appellants find absolutely no mention of a payload, authenticating a payload or checking a payload for conformance to a set of protocols within the cited passage, or anywhere else within the teachings of Ellis. Accordingly, Ellis cannot be relied upon, nor can he combined with the remaining cited art, to provide teaching or suggestion for all limitations of dependent claims 13 and 18.

- 2. The cited art fails to teach or suggest a method for identifying and binding a process, where the method includes evaluating a payload by compiling a profile of the process execution.**

Dependent claims 14 and 19 recite "[t]he method as recited in claim 12, wherein evaluating a payload comprises compiling a profile of the process [agent] execution." Statements in the Final Office Action admit "Kraft and May do not expressly disclose evaluating a payload comprises compiling a profile of the process execution." (Final Office Action, page 6). However, further statements in the Final Office Action suggest that "Ellis teaches this limitation (col. 10, lines 34-55). The Appellant respectfully disagrees, for at least the reasons set forth in more detail below.

The Examiner suggests that teaching for the abovementioned limitation may be found in column 10 of Ellis. The cited passage suggests that a PC user may be granted access or service based on the user's limits, such as resources, credit balance with a service provider, credit history, and whether or not the user's hardware is owned or leased. (col. 10, lines 34-55). Appellants find absolutely no mention of evaluating a payload or compiling a profile of the process execution [of a task] within the cited passage, or anywhere else within the teachings of Ellis. Accordingly, Ellis cannot be relied upon, nor can he be combined with the remaining cited art, to provide teaching or suggestion for all limitations of dependent claims 14 and 19.

- 3. The cited art fails to teach or suggest a method for identifying and binding a process, where the method includes evaluating a payload by simulating the execution of a process.**

Dependent claims 15 and 20 recite "[t]he method as recited in claim 12, wherein evaluating a payload comprises simulating the execution of the process [agent]." Statements in the Final Office Action admit "Kraft and May do not expressly disclose evaluating a payload comprises simulating the execution of the process." (Final Office Action, page 7). However, further statements in the Final Office

Action suggest that "Ellis teaches this limitation (col. 10, lines 9-23). The Appellant respectfully disagrees, for at least the reasons set forth in more detail below.

The Examiner suggests that teaching for the abovementioned limitation may be found in column 10 of Ellis. The cited passage suggests that a meter (10, Fig. 3) could be used to estimate the amount of network resources needed to fulfill a processing request and the associated projected cost. (col. 10, lines 9-23). However, Appellants find absolutely no mention of a payload, evaluating a payload or simulating the execution of the process execution [of a task] within the cited passage, or anywhere else within the teachings of Ellis. Accordingly, Ellis cannot be relied upon, nor can he be combined with the remaining cited art, to provide teaching or suggestion for all limitations of dependent claims 14 and 19.

### Conclusion

As explained in Arguments 1-3 above, the limitations of claims 13-16 and 18-20 are not taught or suggested by Ellis. For at least these reasons, claims 13-16, 18-20 and all claims dependent thereon, are patentably distinct from Ellis. Accordingly, the §103(a) rejection of claims 13-16 and 18-24 is asserted to be erroneous.

### CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-3 and 5-26 was erroneous, and reversal of the decision is respectfully requested. The Commissioner is authorized to charge any required fees to deposit account no. 09-0447.

Respectfully submitted,



Kevin I. Daffer  
Reg. No. 34,146  
Attorney for Appellant

Daffer McDaniel, LLP  
P.O. Box 684908  
Austin, TX 78768-4908  
Date: October 4, 2005  
JMI'

**VIII. CLAIMS APPENDIX**

The present claims on appeal are as follows.

1. A system for identifying and binding a process, said system comprising a network server adapted to receive a payload from a network client over a network, wherein the payload comprises a request for process execution associated with a task, and wherein the server is further adapted to evaluate the payload, create an agent from the payload, and forward the agent to a network host, unknown to and dissimilar from the network client, for process execution associated with the agent.
2. The system as recited in claim 1, wherein the network is a heterogeneous network.
3. The system as recited in claim 1, wherein the heterogeneous network comprises a network of computational devices.
5. The system as recited in claim 3, wherein the network of computational devices comprises a network of multiple platforms.
6. The system as recited in claim 1, wherein the network server comprises a computational device.
7. The system as recited in claim 6, wherein the network server comprises;  
  
a processor;  
  
a storage device;  
  
an evaluating program, wherein the evaluating program is adapted to analyze the payload; and  
  
a binding program, wherein the binding program is adapted to create an agent from the payload.
8. The system as recited in claim 1, wherein the payload comprises:  
  
a set of programming instructions, wherein the set of programming instructions are associated with the process execution; and  
  
a data set, wherein the data set is associated with the process execution.

9. The system as recited in claim 8, wherein the payload further comprises:
- a set of security permissions, wherein the set of security permissions are associated with the process execution; and
  - a financial data set, wherein the financial data set is associated with the process execution.
10. The system as recited in claim 1, wherein the agent comprises the payload containing programming instructions which, when executed by the server, a software data set is requested and configured to provide the payload the ability to perform the process execution.
11. The system as recited in claim 10, wherein the software data set comprises:
- a set of functional parameters;
  - a set of software libraries; or
  - a set of activating programming instructions.
12. A method of identifying and binding a process, said method comprising:
- receiving a payload on a network server from a network client, wherein the payload comprises a request for process execution;
  - evaluating the payload; and
  - creating a process from the payload and forwarding the process to a network host unknown to and dissimilar from the network client.
13. The method as recited in claim 12, wherein evaluating a payload comprises authenticating the payload and checking the payload for conformance to a set of protocols.
14. The method as recited in claim 12, wherein evaluating the payload comprises compiling a profile of the process execution.

15. The method as recited in claim 12, wherein evaluating the payload comprises simulating the execution of the process.
16. The method as recited in claim 15, wherein simulating the execution of the process comprises creating a portion of the process and executing it.
17. A method of identifying and binding a process, said method comprising:  
  
receiving a payload on a network server from a network client, wherein the payload comprises a request for process execution;  
  
evaluating the payload; and  
  
creating an agent from the payload and forwarding the agent to a network host unknown to and dissimilar from the network client.
18. The method as recited in claim 17, wherein evaluating a payload comprises authenticating the payload and checking the payload for conformance to a set of protocols.
19. The method as recited in claim 17, wherein evaluating the payload comprises compiling a profile of the agent execution.
20. The method as recited in claim 17, wherein evaluating the payload comprises simulating the execution of the agent.
21. The method as recited in claim 20, wherein simulating the execution of the process comprises creating a portion of the agent and executing it.
22. The method as recited in claim 20, wherein simulating the execution of the process comprises creating a single agent and executing it.
23. The method as recited in claim 22, wherein creating an agent comprises merging the payload with a software data set that is configured to provide the payload the ability to perform the process execution.

24. The method as recited in claim 23, wherein the software data set comprises a set of functional parameters; a set of software libraries; or a set of activating programming instructions.

25. A computer-usable carrier medium, comprising:

first programming instructions executable on a computational device coupled between a network client and network host maintained anonymous from each other for receiving a payload from the network client, wherein the payload comprises a request for process execution associated with a task;

second programming instructions executable on the computational device for evaluating the payload; and

third programming instructions executable on the computational device for creating a process from the payload, wherein the process is adapted to execute the requested processing on the network host to perform the task.

26. A computer-usable carrier medium, comprising:

first programming instructions executable on a computational device coupled between a network client and network host maintained anonymous from each other for receiving a payload from the network client, wherein the payload comprises a request for process execution;

second programming instructions executable on the computational device for evaluating the payload; and

third programming instructions executable on the computational device for creating an agent from the payload, wherein the agent is adapted to execute the requested processing on the network host.

**IX. EVIDENCE APPENDIX**

No evidence submitted pursuant to §§ 1.130, 1.131, or 1.132 of this title has been entered during the prosecution of the captioned case. In addition, no evidence has been entered by the examiner.

**X. RELATED PROCEEDINGS APPENDIX**

No other prior and pending appeals, interferences, or judicial proceedings are known to Appellant or Assignee which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.